Defence Research and Development Canada
Recherche et développement pour la défense Canada

Review of Existing Wormhole Attack Discovery Techniques

Maria Alexandrovna Gorlatova

Defence R&D Canada – Ottawa
CONTRACT REPORT
DRDC Ottawa CR 2006-165
August 2006

Canada

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
AUG 2006	**N/A**	**-**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Review of Existing Wormhole Attack Discovery Techniques	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Defence R&D Canada - Ottawa Technical Memorandum DRDC Ottawa TM 2006-165 Canada**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES
The original document contains color images.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**SAR**	**32**	

Review of Existing Wormhole Attack Discovery Techniques

Maria Alexandrovna Gorlatova

School of Information Technology and Engineering
University of Ottawa
800 King Edward Avenue
Ottawa, Ontario K1N 6N5
Tel: (613) 562-5738 Fax: (613) 562-5664

Project Manager: Dr. Ramiro Liscano

Contract Number: W7714-050929

Contract Scientific Authority: Dr. Peter C. Mason

Defence R&D Canada – Ottawa

Contractor Report

DRDC Ottawa CR 2006-165

August 2006

Abstract

In this report, we describe a severe Mobile Ad Hoc Network (MANET) routing attack called a wormhole attack and review state-of-the-art ways to thwart wormhole attacks.

In a wormhole attack, intruders tunnel the data from one end of the network to the other, leading distant network nodes to believe they are neighbours and making them communicate through the wormhole link. Unlike many other attacks on ad hoc routing, a wormhole attack can not be prevented with cryptographic solutions because intruders neither generate new, nor modify existing, packets, but rather forward existing ones.

Résumé

Dans le présent rapport, nous décrivons l’attaque par tunnel ver, soit une grave attaque liée à l’acheminement dans le réseau ad hoc mobile (MANET). Nous y offrons aussi des méthodes perfectionnées pour la contrer.

Dans une attaque par tunnel ver, les intrus accèdent aux données par effet tunnel d’une extrémité à l’autre du réseau, ce qui laisse croire aux nuds réseau distants que les intrus sont voisins. Ceux-ci communiquent alors grce à la liaison par tunnel ver. Contrairement à de nombreuses autres attaques menées contre un acheminement spécial, une attaque par tunnel ver ne peut être prévenue au moyen de solutions de chiffrement, car les intrus ne génèrent pas de nouveaux paquets ni ne modifient ceux existants. En effet, ils transmettent plutôt les paquets existants.

This page intentionally left blank.

Executive summary

Attacks, such as the wormhole attack described in this work, can be launched without regard for most network encryption and authentication techniques. For MANETs, the dynamic membership and topology, as well as its open medium, make it vulnerable to wormhole attacks and make detection difficult.

The majority of researchers working in this area try to prevent wormholes by distance-bounding techniques that allow nodes to determine whether the node they receive a message from is close to them. These distance-bounding techniques can be based on geographical information, directional antennas, or on message traveling time information. Although such techniques are analytically sound, they generally require specialized hardware and may not be presently practical. Among them, GPS-based solutions are the most promising.

A number of researchers have proposed to treat wormholes as misbehaving links. Such approaches, however, do not deal with wormholes that are created for reasons other than packet flow disruption, and do not fully address the wormhole attack problem. Finally, several researcher proposed different specialized wormhole detection techniques aimed at specific networks, such as sensor network visualization, or abnormal link frequency in multipath on-demand routing. Such techniques, although limited in scope, do add to the body of knowledge in the wormhole attack prevention area.

Overall, while a number of techniques have been proposed to combat wormhole attacks, an easy, standard, lightweight, versatile, and general solution is still lacking.

Maria Alexandrovna Gorlatova. 2006. Review of Existing Wormhole Attack Discovery Techniques. DRDC Ottawa CR 2006-165. Defence R&D Canada - Ottawa.

Sommaire

Les attaques, comme l'attaque par tunnel ver qui est décrite dans le présent travail, peuvent tre lances sans égard à la plupart des techniques de chiffrement et d'authentification en vigueur. Le MANET ou réseau ad hoc mobile, du fait de sa composition dynamique et de sa topologie ainsi que de son architecture ouverte, est vulnérable aux attaques par tunnel ver. Par ailleurs, il est difficile d'y détecter pareilles attaques.

Les chercheurs uvrant dans ce domaine tentent pour la plupart de prvenir les tunnels ver grce à des techniques de délimitation des distances. Celles-ci permettent aux nuds de dterminer si le nud duquel ils reoivent un message se trouve prè s d'eux. Ces techniques peuvent tre fondées sur de l'information géographique, des antennes directives ou la durée en transit des messages. Malgré que ces techniques permettent de procéder à une analyse approfondie, elles exigent en général du matériel spécialisé et peuvent ne pas s'avérer pratiques actuellement. Parmi ces techniques, les solutions fondées GPS donnent, par ailleurs, les résultats les plus prometteurs.

Un certain nombre de chercheurs ont proposé de traiter les tunnels ver comme des liens au comportement douteux. Toutefois, ces dmarches ne permettent pas de couvrir les tunnels ver créés à d'autres fins que l'interruption de paquets. Aussi, elles ne corrigent pas entirement le problme lié à ces attaques. Enfin, plusieurs chercheurs ont suggéré diverses techniques spécialises de détection de tunnels ver pour des réseaux prcis. Ils ont ainsi mis de l'avant des solutions comme la visualisation de réseaux de capteurs ou le suivi du taux de liens anormaux dans un acheminement sur demande chemins multiples. De telles techniques, malgré que leur portée soit limitée, s'ajoutent à la base de connaissances en matire de prévention des attaques par tunnel ver.

Globalement, mme si un certain nombre de techniques ont été proposées pour lutter contre les attaques par tunnel ver, il manque quand mme à ce sujet une solution générale, polyvalente, légère, standard et facile d'emploi.

Maria Alexandrovna Gorlatova. 2006. Review of Existing Wormhole Attack Discovery Techniques. DRDC Ottawa CR 2006-165. R&D pour la défense Canada - Ottawa.

Table of contents

List of figures

1. Introduction

Mobile wireless ad hoc networks are a relatively new field of research. Such networks are fundamentally different from wired networks, as they use wireless medium to communicate, do not rely on fixed infrastructure, and can arrange themselves into a network quickly and efficiently. In a Mobile Ad Hoc Network (MANET), each node serves as a router for other nodes, which allows data to travel, utilizing multi-hop network paths, beyond the line of sight without relying on wired infrastructure.

MANETs are particularly attractive for situations where deployment of infrastructure is costly or impossible, such as military deployments, emergency rescue operations, and short-lived conference or classroom activities. Security of such networks, however, is a great concern [1]. The open nature of the wireless medium makes it easy for outsiders to listen to network traffic or interfere with it. Lack of centralized control authority makes deployment of traditional centralized security mechanisms difficult, if not impossible. Lack of clear network entry points also makes it difficult to implement perimeter-based defence mechanisms such as firewalls. Finally, in a MANET nodes might be battery-powered and might have very limited resources, which may make the use of heavy-weight security solutions undesirable ([1], [2], [3]).

A large number of routing protocols for MANETs have been proposed to enable quick and efficient network creation and restructuring. However, common ad hoc routing protocols were not designed with security in mind, and assume trusting and cooperative environment [1]. Security of MANET routing is an active research area at this time.

A research field related to MANETs is sensor networks, whose security is also of a great interest. Just like ‘full-scale’ MANETs, sensor networks do not rely on fixed infrastructure, use wireless media to communicate, and serve as routers for each other. However, sensor networks also have peculiarities not shared with general MANETs. Sensors are, in general, extremely resource-constrained, and may have shorter communication range. In addition, sensor networks are often presumed to be dense, marginally (if at all) mobile, and be reporting to a centralized controller.

1.1 Wormhole attack

A wormhole attack is a particularly severe attack on MANET routing where two attackers, connected by a high-speed off-channel link, are strategically placed at different ends of a network, as shown in Figure 1. These attackers then record the wireless data they overhear, forward it to each other, and replay the packets at the other end of the network. Replaying valid network messages at improper places, wormhole attackers can make far apart nodes believe they are immediate neighbours, and force all communications between affected nodes to go through them.

In general, ad hoc routing protocols fall into two categories: *proactive routing protocols* that rely on periodic transmission of routing updates, and *on-demand routing*

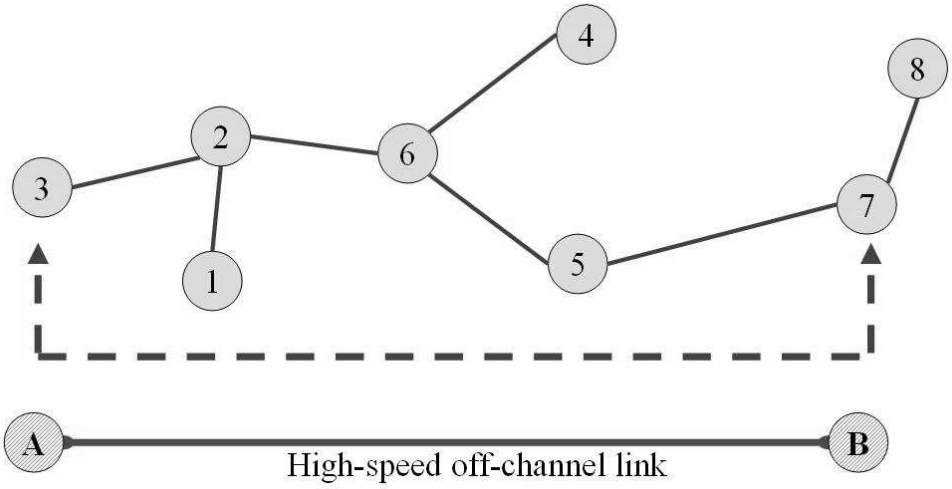

Figure 1: *A network under a wormhole attack. Intruders A and B are connected by an off-channel link (i.e. wired or satellite link), which they use to tunnel network data from one end of the network to the other. Without a wormhole, nodes 7 and 3 are 4 hops apart, - their messages to each other should go through nodes 2, 6, and 5. When intruders A and B activate a wormhole, nodes 7 and 3 are able to directly overhear each others' messages, and are lead to believe they are immediate neighbours. Once this happens, all further communications between nodes 3 and 7 will be going through the wormhole link introduced by A and B.*

protocols that search for routes only when necessary. A wormhole attack is equally dangerous for both proactive and on-demand protocols [2].

When a *proactive routing protocol*, such as Optimized Link-State Routing (OLSR) [4] is used, ad hoc network nodes send periodic HELLO messages to each other indicating their participation in the network. In Figure 1, when node 3 sends a HELLO message, intruder A forwards it to the other end of the network, and node 7 hears this HELLO message. Since 7 can hear a HELLO message from 3, it assumes itself and node 3 to be direct neighbours. Thus, if 7 wants to forward anything to 3, it will do so through the wormhole link, effectively giving the wormhole attackers full control of the communication link.

If a network uses an *on-demand routing protocol*, such as Ad-hoc On-Demand Vector routing (AODV) [5], the wormhole is just as effective. In on-demand protocols, when a node wants to communicate with another node, it floods its neighbours with requests, trying to determine the shortest path to the destination. In Figure 1, if 3 wants to communicate with 7, it sends out a request, which a wormhole, once again, forwards without change to the other end of the network, - directly to node 7. A request also travels along the network in a proper way, so 7 is lead to believe it has two possible routes to node 3: a 4-hop route through nodes 2,6,and 5, and a single-hop direct link. Protocols will then select the shortest route, once again giving wormhole attackers full control of the link.

Majority of ad hoc routing protocols rely on the correctness of their neighbours' information for routing decisions, thus allowing wormhole-induced disruptions to have greater effects. For example, in the situation described in Figure 1, where nodes 3 and 7 think they are direct neighbours, nodes 5 and 8 will then think they are two hops away from node 3 (going through node 7), and will communicate with node 3 through the wormhole link as well.

Once the wormhole attackers have control of a link, they can do a number of things to actively disrupt the network. Attackers can drop the packets their link is supposed to be forwarding. They can drop all packets, a random portion of packets, or specifically targeted packets[1]. Attackers can also forward packets out of order or 'switch' their link on and off.

It should, however, be noted that wormholes are dangerous by themselves, even if attackers are diligently forwarding all packets without any disruptions, - on some level, providing a communication service to the network. With wormholes in place, affected network nodes do not have a true picture of the network, which may disrupt the localization-based schemes, lead to the wrong decisions, etc. Wormholes can also be used to simply aggregate a large number of network packets for the purpose of traffic analysis or encryption compromise. Finally, a wormhole link is simply unreliable, as there is no way to predict what the attackers can do and when. Simply put, the wormholes are compromising network security whether they are actively disrupting routing or not.

2. Solutions to wormhole attacks

Routing security in ad hoc networks is often equated with strong and feasible node authentication and lightweight cryptography. A wide variety of secure extensions to existing routing protocols have been proposed over the years. However, the majority of these protocols are focused on using cryptographical solutions to prevent unauthorized nodes from creating seemingly valid packets [1]. Unfortunately, the wormhole attack can not be defeated by cryptographical measures, as wormhole attackers do not create separate packets - they simply replay packets already existing on the network, which pass all cryptographic checks.

Virtually all generalized secure extensions proposed for currently popular routing protocols do not alleviate wormhole attacks. However, since wormhole attack such a severe thread to ad hoc network security, several researchers have worked on preventing or detecting wormhole attacks specifically. In this section, we summarize and discuss their efforts. In section 2.1, we discuss a technique called 'packet leashes', which allows to prevent packets from traveling farther than radio transmission range.

[1]Two distinct situations are possible here. When no encryption is used, attackers know exactly what they are forwarding, and can target specific packets. When strong multi-layer encryption is used, attackers can either drop packets at random, or try to figure out (based on traffic patterns, packet sizes, etc.) what they are going to drop

Section 2.2 talks about wormhole prevention methods that rely on round trip message time (RTT) to ensure nodes claiming to be located close together really are. In section 2.3, we discuss the work of researchers who, instead of treating wormholes, treat the network disruptions they introduce. Finally, section 2.4 summarized other, more specialized wormhole detection or prevention techniques suitable for only particular kinds of networks.

2.1 Packet leashes

Perhaps the most commonly cited wormhole prevention mechanism is 'packet leashes' by Hu et al ([6], [7]). Hu proposes to add a secure 'leash' containing timing and/or Global Positioning System (GPS) information to each packet on a hop-by-hop basis. Based on the information contained in a packet leash, a node receiving the packet would be able to determine whether the packet has traveled a distance larger than physically possible.

Hu proposes two different kinds of leashes: *geographical leashes* and *temporal leashes*. Geographic leashes require each node to have access to up-to-date GPS information, and rely on loose (in the order of ms) clock synchronization. When geographical leashes are used, a node sending a packet appends to it the time the packet is sent t_s and its location p_s. A receiving node uses its own location p_r and the time it receives a packet t_r to determine the distance the packet could have traveled. Keeping in mind maximum possible node velocity v, clock synchronization error Δ, and possible GPS distance error σ, the distance between the sender and the receiver d_{sr} is upper-bounded by:

$$d_{sr} < \|p_s - p_r\| + 2v(t_r - t_s + \Delta) + \sigma \quad (1)$$

Geographical leashes should work fine when GPS coordinates are practical and available. However, modern GPS technology has significant limitations that should not be overlooked. While the price of GPS devices is going down, it remains substantial. Besides, GPS is somewhat of a nuisance for personal laptops. Also, while, as Hu [6] specifies, it is possible to achieve GPS precision of about 3m with state-of-the-art GPS devices, consumer-level devices do not get (and do not require) this level of resolution. Finally, GPS systems are not versatile, as GPS devices do not function well inside buildings, under water, in the presence of strong magnetic radiation, etc.

As opposed to geographical leashes, *temporal leashes* require much tighter clock synchronization (in the order of nanoseconds), but do not rely on GPS information. When temporal leashes are used, the sending node specifies the time it sends a packet t_s in a packet leash, and the receiving node uses its own packet reception time t_r for verification . In a slightly different version of temporal packet leashes, the sending node calculates an expiration time t_e after which a packet should not be accepted, and puts that information in the leash. To prevent a packet from traveling farther than distance L,

the expiration time is set to:

$$t_e = t_s + \frac{L}{c} - \Delta \tag{2}$$

where c is the speed of light and Δ is the maximum clock synchronization error.

The level of time synchronization required for temporal leashes (on the order of nanoseconds) entails the use of specialized hardware not currently practical in wireless ad hoc networks. In sensor networks, such levels of synchronization are impossible [6] at this time. Temporal packet leashes thus offer an elegant but not practical solution to wormhole attacks.

Wang [8] proposes an approach inspired by packet leashes [6], but based on end-to-end location information, rather than hop-by-hop leashes in [6]. Similar to geographic packet leashes, Wang's method requires each node to have access to up-to-date GPS information, and relies on loosely synchronized clocks. In Wang's approach, each node appends its location and time to a packet it is forwarding, and secures this information with an authentication code. The packet's destination node then verifies the nodes' coordinates (i.e. verifies that reported coordinates are within the communication range) and speeds. A minor disadvantage of this approach is that the end node is left to do all verification. Just like geographical packet leashes proposed by Hu, this approach should work fine where GPS coordinates are appropriate.

2.2 Time-of-flight

Another set of wormhole prevention techniques, somewhat similar to temporal packet leashes [6], is based on the time of flight of individual packets. Wormhole attacks are possible because an attacker can make two far-apart nodes see themselves as neighbours. One possible way to prevent wormholes, as used by Capkun et al [9], Hu et al [10], Hong et al [11], and Korkmaz [12], is to measure round-trip travel time of a message and its acknowledgement, estimate the distance between the nodes based on this travel time, and determine whether the calculated distance is within the maximum possible communication range.

The basis of all these approaches is the following. The Round Trip Travel Time (RTT) δ of a message in a wireless medium can, theoretically, be related to the distance d between nodes, assuming that the wireless signal travels with a speed of light c:

$$d = \frac{\delta * c}{2} \tag{3}$$

$$\delta = \frac{2d}{c} \tag{4}$$

The neighbour status of nodes is verified if d is within the radio transmission range R :

$R > d$ (d within transmission range) $\Rightarrow$

$$R > \frac{\delta * c}{2} \Rightarrow \tag{5}$$

$$\delta < \frac{2R}{c} \tag{6}$$

In essence, the use of RTT eliminates the need for tight clock synchronization required in temporal leashes: a node only uses its own clock to measure time. However, this approach, while accounting for message propagation, completely ignores message processing time. When a message is sent by one node and is acknowledged by another, the time it takes for a node to process a message and to reply to it is generally non-negligible, particularly in the context of bounding short distances using signals whose speed is similar to that of light in vacuum. After all, it takes the light less than 0.2 seconds to circle the entire Earth around the equator. Outstanding clock precision and practically nonexistent errors are required to bound distances on the order of hundreds of meters.

When a de-facto standard of wireless ad hoc networks 802.11 Medium Access Control (MAC) protocol [13] is used, such calculations are downright impossible. 802.11 imposes a short wait time of 10μs (SIFS[2]) between the reception of a packet and sending of 802.11 acknowledgement. When 802.11 is used, transmission range R is generally about 300 meters. The speed of light c is 300,000,000 m/second. Then, from equation 4:

$$\delta = \frac{2d}{c} = \frac{600\,m}{300,000,000\,m/s} = 0.000002s = 2 * 10^{-6} = 2\mu s \tag{7}$$

Therefore, the RTT is an order of magnitude smaller than the delay required by the protocol. We could, of course, account for this processing time by modifying formula 4 in the following manner:

$$\delta = \frac{2d}{c} + S \tag{8}$$

where S is SIFS. However, note that wormhole attackers are not limited by the rules of the network, and could, with some ingenuity, send their packets without 802.11-imposed delay - thus breaking this type of defence altogether. On the other hand, if nodes were to use formula 4 directly, they would have to ignore 802.11-mandated delays, thus breaking it altogether. Hence, in order to use the approaches based on time of flight, special arrangements are required.

[2]This wait time is Short Interframe Space (SIFS) . The SIFS value depends on the version of 802.11 protocol. 802.11a specifies SIFS of 16μs, 802.11b and 802.11g - 10μs[13]

Capkun et al [9] propose to use specialized hardware that enables fast sending of one-bit challenge messages without CPU involvement, as to minimize all possible processing delays. To verify distance between the nodes, each node sends a one-bit challenge to the nodes it 'encounters', and waits for a response. A receiving node immediately sends a single-bit reply. While Capkun's use of specialized hardware is somewhat discouraging, his method is nonetheless very interesting.

Hu [10] proposes a mechanism very similar to Capkun's [9], but does not use single-bit challenge approach. Instead, Hu relies round-trip travel time of full packets with CPU involvement, explicitly assuming medium access delays to be negligible. In addition, Hu's approach requires substantial processing of messages: upon the reception of a message, a node verifies the message correctness (i.e. performs one hash function operation) and sends an authenticated reply. Hong [11] uses a mechanism practically identical to Hu's: upon reception of a HELLO packet, the receiving node sends a probe to the HELLO's sender. When receiving a probe, a node answers it immediately[3].

Korkmaz [12] studied in detail the distance-bounding techniques described by other authors. Korkmaz found that using round-trip time may lead to a high percentage of valid neighbours being rejected. He noted that although a wireless signal is akin to light signal in vacuum, it is not exactly same, and its speed is slower [12]. He also notes that even small errors in measuring time delays alter the distance measurements significantly, as we've alluded to above.

Korkmaz proposes a modified statistical method based on RTT δ. He suggests using two different bounds for RTT, one based on the speed of light c ($boundC = \frac{2R}{c}$), and another based on experimentally determined speed of travel of the wireless signal s ($boundS = \frac{2R}{s}$). If RTT δ is under $\frac{2R}{c}$, the nodes are considered neighbours. If δ is larger than $\frac{2R}{s}$, the nodes are considered non-neighbours. For the nodes with δ in between these bounds, Korkmaz suggests a probabilistic measure of 'neighbourness'. In addition, Korkmaz also proposes to use received signal strength to verify the 'neighbourness' determined from the time of flight. In summary, Korkmaz's approach modifies and extends the RTT-based technique described above.

Approaches based on RTT of a packet are similar in nature to temporal packet leashes, [7], but do not require clock synchronization between nodes. The idea of these approaches is very simple: wireless nodes that claim to be neighbours should be physically close to each other, and when one node sends a packet to another, the answer should arrive very shortly, ideally within the amount of time a wireless signal would travel between the nodes. If there is a wormhole attacker involved, packets end up traveling farther, and thus can not be returned within a short time.

It is intriguing that while Capkun [9] proposes to use special hardware to drive the message processing time down, Hu [10] and Hong [11] simply assume MAC delays to

[3] We have substantial concerns about originality Hong's paper, but nonetheless mention it here for completeness. Hong's wormhole discovery technique ([11], 2005) is for all intents and purposes identical to Hu's work published two years prior to 2005 ([10], 2003). Hong, however, does not acknowledge or even cite Hu's work.

be negligible, and claim the possibility of lightening fast message processing.

It would be very interesting to see one of these schemes implemented on a real-world system. Above, we demonstrated that RTT-based approaches are incompatible with the standard 802.11 MAC protocol. Thus, on top of possibly requiring specialized hardware, these approaches also prohibit the use of the standard MAC protocol, and, overall, do not seem practical.

2.3 Wormhole discovery from wormhole's effect

Several researchers worked on the wormhole attack problem by treating a wormhole as a misbehaving link. In such approaches, a wormhole attack is not specifically identified. Rather, the wormhole's destructive behaviour is mitigated.

Baruch [14] and Chigan [15] use link rating schemes to prevent blackhole and wormhole attacks. They both rely on authenticated acknowledgements of data packets to rate links: if a link is dropping packets, the acknowledgements do not get through, link is rated low and avoided in the future.

These approaches are geared towards discovery and prevention of only one kind of wormhole behaviour: packet loss. Wormholes can do much more than that: they can send packets out of order, confuse location-based schemes, or simply aggregate packets for traffic analysis. Even the distortion of topology information that a wormhole introduce can be a significant problem in particular networks. The real problem with the wormholes is that unauthorized nodes (wormhole attackers) are able to transmit valid network messages. Techniques based on links' performance may be suitable in certain cases, but they do not fully address the wormhole problem.

Consider the scenario shown in Figure 2. Say that originally intruders are creating a wormhole between nodes A and M. To the network, it seems that nodes A and M are direct neighbours, and the link between them is evaluated using a link rating system. When the rating system determines the link A-M to be lossy, it avoids it - which can be detected by the attackers. They can then simply move on: create a fake link between, say, nodes B and L, or even B and M. Since the methods proposed in [14] and [15] do not differentiate between poorly performing links and wormhole intruders, discovery of a bad link between A and M does not trigger a security investigation, and the attackers can thus indefinitely continue to disrupt the network.

2.4 Specialized techniques

A wide variety of wormhole attack mitigation techniques have been proposed for specific kinds of networks: sensor networks, static networks, or networks where nodes use directional antennas. In this section, we describe and discuss such techniques, commenting on their usability and the possibility of their use in general mobile MANETs.

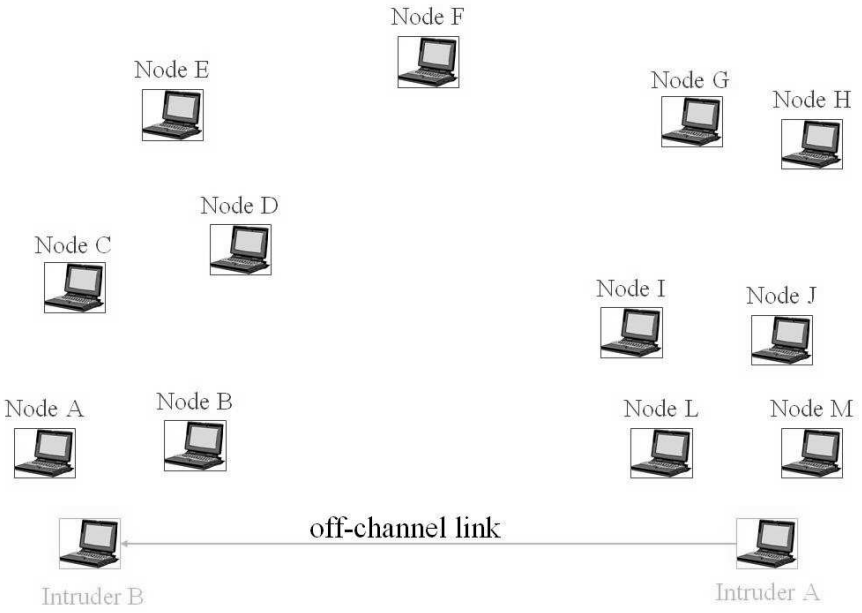

Figure 2: *When a wormhole is treated as a misbehaving link, attackers are not detected and can create wormhole attacks targeting other nodes on the network.*

2.4.1 Nodes with directional antennas

Directional antennas have been extensively studied in the general literature [16]. When directional antennas are used, nodes use specific 'sectors' of their antennas to communicate with each other, as shown in Figure 3. Therefore, a node receiving a message from its neighbour has some information about the location of that neighbour, - it knows the relative orientation of the neighbour with respect to itself, as demonstrated in Figure 3. This extra bit of information makes wormhole discovery much easier than in networks with exclusively omni-directional antennas.

In [16], Hu and Evans propose a solution to wormhole attacks for ad hoc networks in which all nodes are equipped with directional antennas. Wormholes introduce substantial inconsistencies in the network, and can easily be detected. In SERLOC [17], Lazos et al use a slightly different approach. In SERLOC, only a few nodes need to be equipped with directional antennas, but these nodes also have to be location-aware. These nodes then send out localization beacons, based on which regular network nodes determine their own relative location.

The methods proposed by Hu [16] and Lazos [17] are both viable, and could be easily applied to networks that use directional antennas. Currently, such

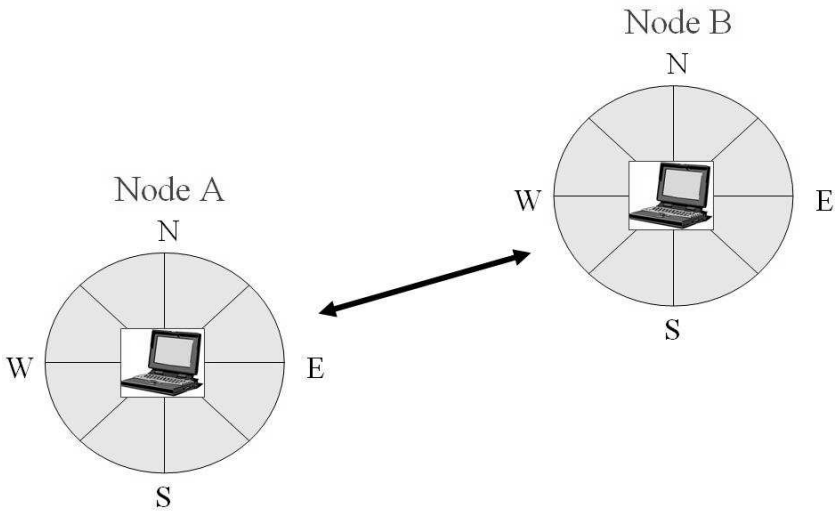

Figure 3: *Nodes using directional antennas. When nodes A and B communicate, they send their messages on specific 'sectors': node A uses its North- East sector, node B - South-West. Therefore both nodes know how they are located with respect to each other. From knowing the sector on which it receives B's messages, A knows that B is located to the North-East. Had nodes A and B used omni-directional antennas, A would not be able to say anything at all about B's location.*

networks are mostly in research stage, and their future prominence is not clear.

2.4.2 Sensor networks: network visualization

Wang and Bhargava [18] introduce an approach in which network visualization is used for discovery of wormhole attacks in stationary sensor networks. In their approach, each sensor estimates the distance to its neighbours using the received signal strength. During the initial sensor deployment, all sensors send this distance information to the central controller, which calculates the network's physical topology based on individual sensor distance measurements. With no wormholes present, the network topology should be more or less flat, while a wormhole would be seen as a 'string' pulling different ends of the network together.

Wang's approach [18] has several aspects that may limit its applicability to general ad hoc networks. Wang assumes a dense sensor network of a polygon shape deployed on a flat surface, - an assumption perhaps justified for sensor networks, but not practical for ad hoc networks. For sparsely located ad hoc network nodes, the estimated physical topology may not be precise. Also, this method requires a central controller, and thus not readily suitable for decentralized networks. Finally, while this method should, theoretically, be extendable to mobile networks, Wang does not study how node mobility would affect the results.

Overall, Wang's method requires more research to be applicable to sparse, decentralized, or mobile ad hoc networks, but seems promising.

2.4.3 Sensor networks: use of location-aware guards

Lazos et al [19] develop a 'graph-theoretical' approach to wormhole attack prevention based on the use of Location-Aware 'Guard' Nodes[4] (LAGNs).

In [19], Lazos uses 'local broadcast keys' - keys valid only between one-hop neighbours - to defy wormhole attackers: a message encrypted with a local key at one end of the network can not be decrypted at another end. However, the establishment of such keys is non-trivial in the possible presence of wormholes. Lazos proposes to use hashed messages from LAGNs to detect wormholes during the key establishment. LAGNs are assumed to be trusted, and, since their location is known, a node can detect certain inconsistencies in messages from different LAGNs if a wormhole is present. Without a wormhole, a node should not be able to hear two LAGNs that are far from each other, and should not be able to hear the same message from one guard twice. Use of LAGNs, in essence, allows the nodes not equipped with GPS devices to perceive network irregularities a wormhole introduces, and to get some idea about their relative position in space.

Lazos's method [19] is elegant. However, it seems more suitable for dense stationary sensor networks than for mobile ad hoc networks[5]. For example, LAGNs in this scheme are assumed to have longer communication range than regular network nodes, - a good assumption for sensor networks (i.e. where sensor motes are regular nodes, laptops are LAGNs), but not usually available with mobile ad hoc networks. Also, the assumption of trusted LAGNs is better justified for sensor networks (where controllers can act as LAGNs) than for standard ad hoc networks. Nonetheless, Lazos' method is relatively lightweight, and may hold promise sensor networks and for particular types of non-sensor ad hoc networks[6] .

2.4.4 Stationary networks: LiteWorp

Khalil et al [20] propose a protocol for wormhole attack discovery in static networks they call LiteWorp. In LiteWorp, once deployed, nodes obtain full two-hop routing information from their neighbours. While in a standard ad hoc routing protocol nodes usually keep track of who their neighbours are, in LiteWorp they also know who the neighbours' neighbours are, - they can take

[4] As we've explained above, Lazos also worked on a wormhole-resistant localization scheme for sensor networks [17], from which this wormhole attack prevention technique seem to directly follow

[5] In the paper, Lazos proposes it for ad hoc networks, but we feel it is more suitable for sensor networks

[6] While the need for specialized high-range location-aware 'guards' is probably limiting for emergency and tactical operations, it may be suitable for a mixed wired/wireless networks (i.e. office networks, rooftop, etc.) where stationary high-power wireless access points may serve as LANGs

advantage of two-hop, rather than one-hop, neighbour information. This information can be exploited to detect wormhole attacks[7].

After authentication, nodes do not accept messages from those they did not originally register as neighbours. Also, nodes observe their neighbours' behaviour to determine whether data packets are being properly forwarder by the neighbour, - a so-called 'watchdog' approach. LiteWorp adds an interesting wormhole-specific twist to the standard watchdog behaviour: nodes not only verify that all packets are forwarded properly, but also make sure that no node is sending packets it did not receive (as would be the case with a wormhole)

LiteWorp is, no doubt, interesting, but would not work at all in a scenario where node mobility is a factor. Since node's neighbours are determined and detected only once in LiteWorp, and the packets from non-neighbouring nodes are rejected, no node movement is allowable. Therefore, LiteWorp is applicable to static networks only[8].

Overall, while this protocols is interesting, it does not seem practical.

2.4.5 Networks with on-demand multipath routing: a statistical analysis approach

Song et al [21] approach the wormhole attack from a different angle. Song proposes a wormhole discovery mechanism based on statistical analysis of multipath routing. Song observes that a link created by a wormhole is very attractive in routing sense, and will be selected and requested (for routing) with unnaturally high frequency. This unusual route selection frequency can be statistically detected and used to identify wormhole links. Such statistical analysis approach is fundamentally different from the majority of others where, in general, wormhole detection is related to locating a node in absolute or relative terms (based on network topology, time of packet transmission, GPS coordinates, with respect to GPS-aware nodes, etc).

Song's method requires neither special hardware nor any changes to existing routing protocols. In fact, it does not even require aggregation of any special information, as it only uses routing data already available to a node. These factors allow for easy integration of this method into intrusion detection systems.

However, Song's method is somewhat limited in scope as it applies only to routing protocols that are both on-demand and multipath. Non-multipath on-demand protocols do not provide enough information for the

[7]To exploit this data fully, LiteWorp packets not only include 'sender' information, but also 'previous hop' information, rarely found in other routing protocols

[8]Note, that for purely static networks there is also a trivial solution to wormhole attacks: static routing

determination of link frequencies. While on-demand routing protocols keep complete information about routes they discover, proactive ones rely on next-hop information, which does not allow the calculation of link frequencies. Nonetheless, within its scope Song's method is very interesting, and could be integrated in a real-world system with little effort.

3. Discussion and summary

Wormhole attacks, in which adversaries tunnel network data from one end of the network to another using an off-channel link, are a severe routing security concern in mobile wireless ad hoc networks. Wormhole attacks can not be prevented by cryptographic measures as in a wormhole attack they attackers do not create any packets themselves, but simply forward the packets they hear coming from valid network nodes.

Possible solutions to wormhole attacks proposed by different researchers are discussed in our report. In the previous sections, we described and discussed all major proposed solutions to wormhole attacks. Brief summary of all approaches described in the previous section is provided in Table 1.

Several researchers use distance-bounding techniques to detect network packets that travel distances beyond radio range, thus preventing packets that have gone through the wormhole from being accepted. However, majority of these techniques rely on specialized hardware, and may not be practical. Of distance-bounding techniques, GPS-based ones are particularly interesting, as, of the specialized hardware proposed to combat wormhole attacks, GPS is perhaps the most general in purpose, most available currently, and overall most promising. The effectiveness of GPS-based wormhole attack solution is intuitively solid: a packet can not travel to another end of the network undetected if all nodes know precisely where they are located and where their neighbours are. Unfortunately, GPS-based wormhole combatting techniques inherit the limitations of GPS technology. They can not be used where GPS does not work (underwater, inside buildings, caves, etc.), or in small sensor networks(due to the resolution of GPS devices).

Nonetheless, GPS-based techniques are interesting, particularly for military or emergency situations, where GPS devices could be used for location awareness purposes, and could be added to network routing without any additional costs.

Network visualization technique presented in [18] for dense sensor networks does not require special hardware, and appears to be very interesting. In this technique, each node reports its perceived distance to its neighbours to a centralized controller. Based on the data collected from network nodes, the controller calculates the estimation of network's physical topology, to which a wormhole, in certain scenarios, introduces impossibilities. It would be very interesting to study how this technique performs on networks that are mobile and not dense. Most likely, the technique will still work, but

perhaps with reduces accuracy and higher false alarm rate. If that is the case, with the use of mobile agents for network visualization instead of the central controller this technique could be applied to general MANETs rather than to sensor networks only.

Finally, the last technique we found particularly interesting is the one based on anomalous frequency of route selection when wormholes are present on a network [21]. This technique, although it applies to multipath on-demand protocols only, is interesting because it is lightweight and, unlike many others, can be easily and immediately integrated into a MANET Intrusion Detection System (IDS). In essence, this technique is akin to those employed by IDS systems in wired networks (for example, on a wired network a port scan can be detected by observing high and abnormal rate of port requests), and could potentially be useful.

Overall, a significant amount of work has been done on solving wormhole attack problem. A standard solution is still lacking, although several very useful solutions applicable to some networks have been described.

[9]These approaches rely on a node immediately answering a challenge message , which is not possible with standard wireless MAC (such as 802.11). It is most likely that enabling immediate replies to messages will require specialized hardware rather than standard wireless cards

Table 1: *Summary of wormhole discovery methods*

Method	Requirements	Commentary
Packet leashes, geographical ([7])	GPS coordinates of every node; Loosely synchronized clocks (ms)	Robust, straightforward solution; inherits general limitations of GPS technology
Packet leashes, temporal ([7])	Tightly synchronized clocks (ns)	**Impractical**; required time synchronization level not currently achievable in to sensor networks
Packet leashes, end-to-end ([8])	GPS coordinates; Loosely synchronized clocks (ms)	Inherits limitations of GPS technology
Time of flight ([9], [10], [11], [12])	Hardware enabling one-bit messages and immediate replies without CPU involvement ([9]); Not clear[9]([10],[11], [12])	**Impractical**; likely to require MAC-layer modifications
Wormhole as a misbehaving link ([14], [15])	none	Addresses packet loss, but does not fully address or prevent wormholes in general
Directional antennas ([16], [17])	Directional antennas on all nodes ([16]) or several nodes with both GPS and directional antennas ([17])	Good solutions for networks relying on directional antennas, but not directly applicable to other networks
Network visualization [18]	Centralized controller	Seems promising; Works best on dense networks; Mobility not studied; Varied terrains not studied
Localization[19]	Location-aware 'guard' nodes	Good solution for sensor networks; Not readily applicable to mobile networks
LiteWorp [20]	none	Applicable only to static stationary networks; **Impractical**
Statistical analysis [21]	no requirements	Works only with multi-path on-demand protocols;

References

1. Security in Mobile Ad Hoc Networks: Challenges and Solutions, Yang, H. and Luo, H. and Ye, F. and Lu, S. and Zhang, U. , Wireless Communications, IEEE, vol. 11, num. 1, pp. 38-47, 2004

2. A Survey of Secure Wireless Ad Hoc Routing, Y.-C. Hu, A. Perrig, Security and Privacy Magazine, IEEE, vol. 2, issue 3, pp. 28-39, May 2004.

3. Intrusion Detection in Wireless Ad Hoc Networks, A. Mishra, K. Nadkarni, A. Patcha, IEEE Wireless Communications, Vol 11, issue 1, pg. 48-60, February 2004

4. IETF draft Optimized Link State Routing (OLSR) protocol, RFC 3626.

5. IEFT draft Ad-Hoc On-demand Distance Vector Routing (AODV) protocol, RFC 3561

6. Packet leashes: a defense against wormhole attacks in wireless networks, Y.-C. Hu, A. Perrig, D. B. Johnson, INFOCOM 2003, Twenty-Second Annual Joint Conference of the IEEE Computer and Communication Societies, Vol. 3, March 30 - April 3rd 2003, pp. 1976-1986

7. Wormhole Attacks in Wireless Networks, Y.-C. Hu, A. Perrig, D. B. Johnson, Selected Areas of Communications, IEEE Journal on, vol. 24, numb. 2, pp. 370-380, 2006

8. Defending against Wormhole Attacks in Mobile Ad Hoc Networks, W. Weichao, B. Bharat, Y. Lu, X. Wu, Wiley Interscience, Wireless Communication and Mobile Computing, January 2006

9. SECTOR: Secure Tracking of Node Encounters in Multi-Hop Wireless Networks, S. Capkun, L. Buttyan, J.-P. Hubaux, October 2003, Processings of the 1st ACM Workshop on Security of Ad Hoc and Sensor Networks

10. Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols, Y-C Hu, A. Perrig, D. Johnson , Wise 2003, September 19, 2003, San Diego, California, USA

11. Secure OLSR, F. Hong, L. Hong, C. Fu, Advanced Information Networking and Applications, AINA 2005, 19th International Conference On, Vol. 1, 25-30, pp. 713-718, March 2005

12. Verifying Physical Presence of Neighbours against Replay-based Attacks in Wireless Ad Hoc Networks, Korkmaz T., Information Technology: Coding and Computing 2005, ITCC 2005, International Conference On, 2005, pp. 704-709

13. Medium Access Control (MAC) and Physical (PHY) Specifications. ANSI/IEEE Std 802.11 , 1999 Edition.

14. On the Survivability of Routing Protocols in Ad Hoc Wireless Networks, A. Baruch, R. Curmola, C. Nita-Rotaru, D. Holmer, H. Rubens, Converence on Security and Privacy for Emerging Areas in Communications, SecureComm 2005, September 2005

15. Secure Node Misbehaviors in Mobile Ad Hoc Networks, C. Chigan, R. Bandaru, Vehicular Technology Conference, 2004, VTC 2004, IEEE 60th, Volume 7, 26-29 Sept. 2004, pp. 4730-4734

16. Using Directional Antennas to Prevent Wormhole Attacks, L. Hu, D. Evans, Proceedings of the 11th Network and Distributed System Security Symposium, pp. 131-141, 2003

17. Serloc: Secure Range-Independent Localization for Wireless Sensor Networks, L. Lazos, R. Poovendran, Proceedings of the ACM Workshop on Wireless Security, pp. 21-30, October 2004.

18. Visualization of wormholes in sensor networks, W. Wang, B. Bhargava., Proceedings of the 2004 ACM workshop on Wireless Security, pp. 51-60, 2004.

19. Preventing Wormhole Attacks on Wireless Ad Hoc Networks: a Graph Theoretical Approach, L. Lazos, R. Poovendram, C. Meadows, P. Syverson, L.W. Chang, IEEE Communication Society, WCNC 2005

20. A Lightweight Countermeasure for the Wormhole Attack in Multihop Wireless Networks, I. Khalil, S. Bagchi, N. B. Shroff, Proceedings of the 2005 International Conference on Dependable Systems and Networks (DSN'05)

21. Wormhole Attack Detection in Wireless Ad Hoc Networks: a Statistical Analysis Approach, N. Song, L. Qian, X. Li, Parallel and Distributed Processing Symposium, 2005, Proceedings of, 19th IEEE International IPDPS'05, 04-08 April 2005, pp.

22. Low-cost Attacks against packet Delivery, Localization, and Time Synchronization Services in Under-Water Sensor Networks, Kong, J. and Ji, Z. and Wang, W. and Gerla, M. and Bagrodia, R. and Bhargava, B, Proceedins of the ACM Workshop on Wireless Security, pp. 87-96, WiSe'05, September 2005

List of Acronyms

AODV Ad-hoc On-Demand Vector routing

GPS Global Positioning System

IDS Intrusion Detection System

IP Internet Protocol

LAGN Location-Aware Guard Node

MAC Medium Access Control

MANET Mobile Ad Hoc Network

OLSR Optimized Link-State Routing

RTT Round Trip Travel Time

SIFS Short Interframe Space

DOCUMENT CONTROL DATA

(Security classification of title, body of abstract and indexing annotation must be entered when the overall document is classified)

1. ORIGINATOR (the name and address of the organization preparing the document. Organizations for whom the document was prepared, e.g. Establishment sponsoring a contractor's report, or tasking agency, are entered in section 8.)

School of Information Technology and Engineering
University of Ottawa
800 King Edward Avenue, Ottawa ON K1N 6N5

2. SECURITY CLASSIFICATION (overall security classification of the document, including special warning terms if applicable)

UNCLASSIFIED

3. TITLE (the complete document title as indicated on the title page. Its classification should be indicated by the appropriate abbreviation (S,C or U) in parentheses after the title.)

Review of Existing Wormhole Attack Discovery Techniques (U)

4. AUTHORS (Last name, first name, middle initial)

Gorlatova, M.A.

5. DATE OF PUBLICATION (month and year of publication of document)

August 2006

6a. NO. OF PAGES (total containing information. Include Annexes, Appendices, etc.)

23

6b. NO. OF REFS (total cited in document)

22

7. DESCRIPTIVE NOTES (the category of the document, e.g. technical report, technical note or memorandum. If appropriate, enter the type of report, e.g. interim, progress, summary, annual or final. Give the inclusive dates when a specific reporting period is covered.)

Contractor Report

8. SPONSORING ACTIVITY (the name of the department project office or laboratory sponsoring the research and development. Include the address.)

DRDC Ottawa

9a. PROJECT OR GRANT NO. (if appropriate, the applicable research and development project or grant number under which the document was written. Please specify whether project or grant)

15br01

9b. CONTRACT NO. (if appropriate, the applicable number under which the document was written)

W7714-050929

10a. ORIGINATOR'S DOCUMENT NUMBER (the official document number by which the document is identified by the originating activity. This number must be unique to this document.)

10b. OTHER DOCUMENT NOS. (Any other numbers which may be assigned this document either by the originator or by the sponsor)

DRDC Ottawa CR 2006-165

11. DOCUMENT AVAILABILITY (any limitations on further dissemination of the document, other than those imposed by security classification)

(x) Unlimited distribution
( ) Distribution limited to defence departments and defence contractors; further distribution only as approved
( ) Distribution limited to defence departments and Canadian defence contractors; further distribution only as approved
( ) Distribution limited to government departments and agencies; further distribution only as approved
( ) Distribution limited to defence departments; further distribution only as approved
( ) Other (please specify):

12. DOCUMENT ANNOUNCEMENT (any limitation to the bibliographic announcement of this document. This will normally correspond to the Document Availability (11). However, where further distribution (beyond the audience specified in 11) is possible, a wider announcement audience may be selected.)

13. ABSTRACT (a brief and factual summary of the document. It may also appear elsewhere in the body of the document itself. It is highly desirable that the abstract of classified documents be unclassified. Each paragraph of the abstract shall begin with an indication of the security classification of the information in the paragraph (unless the document itself is unclassified) represented as (S), (C), or (U). It is not necessary to include here abstracts in both official languages unless the text is bilingual).

In this report, we describe a severe Mobile Ad Hoc Network (MANET) routing attack called a wormhole attack and review state-of-the-art ways to thwart wormhole attacks.

In a wormhole attack, intruders tunnel the data from one end of the network to the other, leading distant network nodes to believe they are neighbours and making them communicate through the wormhole link. Unlike many other attacks on ad hoc routing, a wormhole attack can not be prevented with cryptographic solutions because intruders neither generate new, nor modify existing, packets, but rather forward existing ones.

14. KEYWORDS, DESCRIPTORS or IDENTIFIERS (technically meaningful terms or short phrases that characterize a document and could be helpful in cataloguing the document. They should be selected so that no security classification is required. Identifiers such as equipment model designation, trade name, military project code name, geographic location may also be included. If possible keywords should be selected from a published thesaurus. e.g. Thesaurus of Engineering and Scientific Terms (TEST) and that thesaurus-identified. If it is not possible to select indexing terms which are Unclassified, the classification of each should be indicated as with the title.)

Mobile Ad Hoc Network
Wireless Security
Wormhole Attack

Defence R&D Canada

Canada's leader in Defence
and National Security
Science and Technology

R & D pour la défense Canada

Chef de file au Canada en matière
de science et de technologie pour
la défense et la sécurité nationale

www.drdc-rddc.gc.ca